JOURNAL OF ALGEBRA **191,** 371–381 (1997)
ARTICLE NO. JA976869

A Simplicity Criterion for Finite Groups*

Huiwen Deng

Department of Computer Science, Southwest-China Normal University, Chongqing 630715, Peoples Republic of China

Wujie Shi

Institute of Mathematics, Southwest-China Normal University, Chongqing 630715, Peoples Republic of China

Communicated by Gernot Stroth

Received February 14, 1996

Given a finite group G, let $\pi_e(G)$ denote the set of all orders of elements in G. In this paper, we investigate the relation between the number of primes and that of composite numbers in $\pi_e(G)$ and obtain a criterion for the simplicity of finite groups. © 1997 Academic Press

1. INTRODUCTION

Throughout this paper, all groups are finite and all simple groups are nonabelian.

Given a group G, we denote the set of all prime divisors of order G by $\pi(G)$ and the set of all element orders of G by $\pi_e(G)$. Clearly, $\pi(G)$ is the set consisting of primes that lies in $\pi_e(G)$. Usually $|X|$ denotes the number of elements of a set X. For convenience, we define

$$\psi(G) = \text{the number of composite numbers in } \pi_e(G),$$

which in fact is the number of elements of $\pi_e(G) - \pi(G) - \{1\}$. All further unexplained notation is standard and can be found, for example, in [4].

* Project supported by the National Natural Science Foundation of China.

0021-8693/97 $25.00

The groups G such that $\psi(G) = 0$ were classified in [5, 17]. Especially, such a group G satisfies $|\pi(G)| \leq 3$ and if $|\pi(G)| = 3$, then G is a simple group. In [18], it was proved that if $\psi(G) = 1$, then $|\pi(G)| \leq 4$, and further $|\pi(G)| = 4$ only if G is simple. [16] proposed the following

Problem. Let G be a finite group. Does there exist a general relation among $|\pi(G)|$, $\psi(G)$, and the simplicity of G?

In this paper, we solve the problem and prove the following.

THEOREM A. *Suppose that G is simple. Then we have $|\pi(G)| \leq \psi(G) + 3$, and further $|\pi(G)| = \psi(G) + 3$ holds if and only if G is one of the following simple groups.*

I. A_5, $L_2(11)$, $L_2(13)$, $L_2(2^4)$, $L_3(4)$, J_1;

II. $Sz(q)$, *where* $q = 2^{2n+1}$ *satisfies that each of* $q - 1$, $q - \sqrt{2q} + 1$, *and* $q + \sqrt{2q} + 1$ *is either a prime or a product of two distinct primes*;

III. $L_2(2^n)$, *where* n $(n \geq 5)$ *is an odd prime and satisfies both* $(2^n + 1)/3$ *is a prime and* $2^n - 1$ *is either a prime or a product of two distinct primes*;

IV. $L_2(3^n)$, *where n is an odd prime and satisfies both* $(3^n + 1)/4$ *is a prime and* $(3^n - 1)/2$ *is either a prime or a product of two distinct primes*;

V. $L_2(5^n)$, *where n is an odd prime satisfying both* $(5^n - 1)/4$ *and* $(5^n + 1)/6$ *are primes*;

VI. $L_2(p)$, *where p is a prime greater than* 13 *and one of the following holds*

(1) $(p - 1)/4$ *and* $(p + 1)/6$ *are primes*;

(2) $(p - 1)/6$ *and* $(p + 1)/4$ *are primes*.

THEOREM B. *Suppose that G is a finite group. Then, we have an inequality $|\pi(G)| \leq \psi(G) + 3$, and if $|\pi(G)| = \psi(G) + 3$, then G is a simple group.*

We use the classification of all finite simple groups.

2. SEVERAL LEMMAS

Our arguments depend on the prime graph components of simple groups (see [11, 21]). The prime graph $\Gamma(G)$ of a group G is a graph whose vertex set is the set $\pi(G)$ and two distinct primes p, q are linked by an edge if and only if G contains an element of order pq. Denote the connected components of the graph $\Gamma(G)$ by π_i, $i = 1, 2, \ldots, t(G)$, where

$t(G)$ is the number of connected components, and if $|G|$ is even, denote the component containing 2 by π_1.

In fact, π_i $[i = 1, 2, \dots, t(G)]$ are the vertex sets of the connected components of $\pi(G)$. It is clear that $|\pi(G)| = \sum_{i=1}^{t(G)} |\pi_i|$. For every i, since π_i is a connected component, π_i has a spanning tree (a connected graph that contains no cycles is called a tree). It is well known that any tree with n vertices has exactly $n - 1$ edges. Put

$$\psi'(G) = \psi(G) - \sum_{i=1}^{t(G)} (|\pi_i| - 1).$$

Then $\psi'(G)$ is greater than or equal to the number of such composite numbers that are in $\pi_e(G)$, but not equal to pq (p and q are two distinct primes). The following lemma and its corollary are obvious.

LEMMA 1. *For any group G, $|\pi(G)| = \psi(G) + t(G) - \psi'(G)$ holds.*

COROLLARY 2. (1) *If $t(G) \leq 2$, then $|\pi(G)| < \psi(G) + 3$.* (2) *If $t(G) = 3$, then $|\pi(G)| \leq \psi(G) + 3$. Furthermore the equality holds if and only if $\psi'(G) = 0$.*

Next we will prove the following.

LEMMA 3. *Suppose that Γ is a connected graph with n vertices. If we remove m $(m < n)$ vertices from the graph Γ, then we remove m edges at least.*

Proof. Since any connected graph has a spanning tree, we may assume that the graph Γ is tree without loss of generality. The removal of m $(m < n)$ vertices results in a subgraph, which has obviously at most $n - m - 1$ edges. Suppose the conclusion of the lemma were not true. Then the number of edges in Γ is at most $(m - 1) + (n - m - 1) = n - 2$. This contradicts with the fact that Γ has exactly $n - 1$ edges as Γ is a tree by our assumption.

In our proof of Theorem B, we will use the following unpublished result of Gruenberg and Kegel [8].

LEMMA 4 (see [21]). *If G is a group such that $t(G) \geq 2$, then G has one of the following structures*: (1) *Frobenius or 2-Frobenius*, (2) *simple*, (3) *an extension of a π_1-group by a simple group*, (4) *a simple group extended by a π_1-group*, *or* (5) *an extension of a π_1-group by a simple group that itself is extended by a π_1-group*.

A group G is called 2-Frobenius if there exists a normal series $1 \leq H \leq K \leq G$ of G such that H is the Frobenius kernel of K and K/H is the Frobenius kernel of G/H.

The following two results, which can be found in [12], will also be used several times in our proof of Theorem B.

LEMMA 5 (Thompson). *If G admits a fixed-point-free automorphism of prime order, then G is nilpotent.*

LEMMA 6. *Assume that a π-group H acts fixed-point-freely on a nontrivial π'-group G. Then any Sylow subgroup of H is either cyclic or generalized quaternion.*

About the number $t(G)$ of connected components of $\pi(G)$, we prove the following result.

LEMMA 7. *Let G be a group. Suppose that either G is solvable or the Sylow 2-subgroups of G are generalized quaternion. Then $t(G) \leq 2$.*

Proof. (1) When G is solvable, it is almost clear that $t(G) \leq 2$ by [8]. We may prove this as follows. Suppose $t(G) \geq 3$. We could get a set consisting of primes p_i, which is some prime in π_i, $i = 1, 2, \ldots, t(G)$, i.e., $\pi = \{p_i \mid 1 \leq i \leq t(G)\}$. We clearly have that $|\pi| = t(G) \geq 3$. Since G is solvable, G has a Hall π-group H. By our choice of π, H is a group in which every element has prime power order. It is impossible by [9].

(2) Assume that a Sylow 2-subgroup of G is generalized quaternion. By the Brauer–Suzuki theorem [3], $G/O(G)$ has an element of order 2 that lies in its center. Hence $t(G/O(G)) = 1$. Suppose $t(G) \geq 3$. Since $O(G)$ is solvable, $t(O(G)) \leq 2$. Therefore, $t(O(G)) = 2$ and an element of order 2 acts fixed-point-freely on $O(G)$. By Lemma 5, $O(G)$ is nilpotent. So $t(O(G)) = 1$, a contradiction.

3. PROOFS OF THE THEOREMS

Proof of Theorem A. By Corollary 2(1), we may assume that $t(G) \geq 3$. The prime graph components of simple groups are listed in [11, 21]. It is clear that $t(G) \leq 6$ for any group. By our assumption, we will discuss the four cases $t(G) = 6, 5, 4, 3$ separately.

(a) $t(G) = 6$. In this case, G is isomorphic to J_4. From [4], we have $|\pi(J_4)| = 10$ and $\psi(J_4) \geq 8$. Hence, it is clear that $|\pi(J_4)| < \psi(J_4) + 3$ holds.

(b) $t(G) = 5$. From [11, 21], we have that G is isomorphic to $E_8(q)$ for some q. Suppose that W is the Weyl group of G. Then W has a simple section $O_8^+(2)$ (see [1], pp. 228–232). This gives $4, 9, 12 \in \pi_e(G)$ by [4]. Furthermore $\psi'(G) \geq 3$. Hence, we have that $|\pi(G)| \leq \psi(G) + 2$ by Lemma 1. So $|\pi(G)| < \psi(G) + 3$.

(c) $t(G) = 4$. From [11, 21], it is easy to see that G is one of the following simple groups.

(1) $E_8(q)$ for some q;

(2) $Sz(q)$, $q = 2^{2n+1}$;

(3) ${}^2E_6(2)$, $L_3(4)$, M_{22}, J_1, $O'N$, Ly, Fi'_{24}, M.

For group 1, we have that $|\pi(G)| < \psi(G) + 3$ as seen in case b.

Suppose G is Sz(q). Since $4 \in \pi_e(G)$, $|\pi(G)| \leq \psi(G) + 3$ holds by Lemma 1. By [4, 11], $|G| = q^2(q-1)(q - \sqrt{2q} + 1)(q + \sqrt{2q} + 1)$, $\pi_1 = \{2\}$, $\pi_2 = \pi(q-1)$, $\pi_3 = \pi(q - \sqrt{2q} + 1)$, and $\pi_4 = \pi(q + \sqrt{2q} + 1)$. From the structure of G, we know that G contains cyclic Hall π_i-subgroup for $i \geq 2$. The equality $|\pi(G)| = \psi(G) + 3$ forces $\psi'(G) = 1$. Therefore, we have assertion II of Theorem A.

From [4], we may find some information in Table 1 about the simple groups listed in group 3. It is evident from the table that $|\pi(G)| \leq \psi(G) + 3$, and if the equality holds, then G is either $L_3(4)$ or J_1, which are listed in I.

(d) $t(G) = 3$. By Corollary 2(2), the inequality $|\pi(G)| \leq \psi(G) + 3$ always holds, and $|\pi(G)| = \psi(G) + 3$ if and only if $\psi'(G) = 0$. In particular, Sylow 2-subgroups of G are elementary abelian. By [6, p. 485], G is one of the following:

(1) J_1;

(2) a simple group of Ree type;

(3) $L_2(2^n)$, $n \geq 2$;

(4) $L_2(q)$, $q > 3$, $q \equiv 3, 5 \pmod 8$.

Since $t(J_1) = 4$ and since any simple group of Ree type contains an element of order 9 [20], i.e., $\psi'(G) \geq 1$, we exclude cases 1 and 2 immediately.

TABLE 1

Group	$\lvert\pi(G)\rvert$	$\psi(G)$
${}^2E_6(2)$	8	18
$L_3(4)$	4	1
M_{22}	5	3
J_1	6	3
$O'N$	7	10
Ly	8	19
Fi'_{24}	9	25
M	15	57

Suppose that G is isomorphic to $L_2(2^n)$, $n \geq 2$. From [11], we have $\pi_1 = \{2\}$, $\pi_2 = \pi(2^n + 1)$, and $\pi_3 = \pi(2^n - 1)$. Since G contains elements of order $2^n + 1$ and order $2^n - 1$, and since $\psi'(G) = 0$, $2^n + 1$ and $2^n - 1$ are either primes or the product of two distinct primes. First, we assume that n is a composite number. When $n \leq 6$, the group satisfying $\psi'(G) = 0$ must be $L_2(2^4)$, which is listed in I of Theorem A. If $n > 6$, then $2^n + 1$ or $2^n - 1$ contains at least three prime factors. This does not occur. Second, we assume that n is a prime. If $n = 2$, then G is isomorphic to A_5, which is in I. If n is an odd prime, then 3 divides $2^n + 1$. Hence $(2^n + 1)/3$ must be a prime. Of course, $2^n - 1$ may be either a prime or a product of two distinct primes. This is III.

Suppose G is isomorphic to $L_2(q)$, $q > 3$, and $q \equiv 5 \pmod 8$. Put $q = p^n$, $n \geq 1$. From [21], we have $\pi_1 = \pi(q - 1)$, $\pi_2 = \{q\}$, and $\pi_3 = \pi((q + 1)/2)$. That 4 (but 8 does not) divides $q - 1$ implies $q = 4k + 1$, k odd. Since $(q + 1)/2, (q - 1)/2 \in \pi_e(G)$ and $\psi'(G) = 0$, we have that either $k = 1$ or k is an odd prime. When $k = 1$, G is isomorphic to A_5 as $q = 5$. When k is an odd prime, consider

$$4k = q - 1 = (p - 1)\left(p^{n-1} + \cdots + p + 1\right). \tag{$*$}$$

If $n = 1$, then $q = p$ is an odd prime of type $4k + 1$, k an odd prime. Assume that 3 does not divide $q + 1$. Then 3 divides $q - 1$. So $k = 3$, that is, $q = 13$, which is in I. Assume that 3 divides $q + 1$. In this case, we have that both $(q + 1)/6$ and $(q - 1)/4$ are primes. This is the case VI(1). If $n \geq 2$, from the identity $(*)$ we have $p = 3$ or $p = 5$. When $p = 3$, n must be even, and further 8 divides $3^n - 1$, a contradiction. Hence we get $p = 5$. Since 3 divides $5^n + 1$ and $\psi'(G) = 0$, we have that $(5^n - 1)/4$ and $(5^n + 1)/6$ are primes. Clearly, n is an odd prime. This is the case V.

Finally, suppose G is isomorphic to $L_2(q)$, $q > 3$, and $q \equiv 3 \pmod 8$. From [21], we arrive at $\pi_1 = \pi(q + 1)$, $\pi_2 = \{q\}$, and $\pi_3 = \pi((q - 1)/2)$. Since $(q + 1)/2, (q - 1)/2 \in \pi_e(G)$ and $\pi'(G) = 0$, we have $q = 4k - 1$, k an odd prime. If $k = 3$, then G is $L_2(11)$, which is listed in I. Consider the case $k > 3$. That n is even implies 2 divides $(q - 1)/2$, which is a contradiction. When n is odd, we have the identity

$$4k = q + 1 = (p + 1)\left(p^{n-1} - p^{n-2} + \cdots - p + 1\right), \qquad q = n^n. \tag{$**$}$$

If $n = 1$, then $q = p$ is a prime of type $4k - 1$, where k is an odd prime. Clearly, 3 divides $p - 1$. Hence, $(p - 1)/6$ and $(p + 1)/4$ must be primes. This is the case VI(2). If $n \geq 2$, then $p = 3$ from the identity $(**)$. Since $(q + 1)/2, (q - 1)/2 \in \pi_e(G)$, we have that both $(3^n + 1)/4$ is a prime and $(3^n - 1)/2$ is either a prime or a product of two distinct primes. Furthermore, n is an odd prime. This is the case IV of Theorem A.

Remark. In recent years some papers have dealt with the question of characterizing groups G by the set $\pi_e(G)$. For example, in [2, 14] it was proved that if $\pi_e(G) = \pi_e(L_2(q))$, $q \neq 9$, then $G \cong L_2(q)$; if $\pi_e(G) = \pi_e(J_1)$, then $G \cong J_1$. In [15] it was proved that if $\pi_e(G) = \pi_e(\mathrm{Sz}(q))$, then $G \cong \mathrm{Sz}(q)$). An analogous result in the case $\pi_e(G) = \pi_e(L_3(4))$ was proved in [13]. Therefore all these simple groups listed in Theorem A can be characterized only by $\pi_e(G)$.

Next we prove Theorem B.

Proof of Theorem B. Use induction on $|G|$. By Corollary 2(2), we only need to assume that $t(G) \geq 3$. According to Lemma 4, we may divide the proof into five cases.

Case 1. G is either Frobenius or 2-Frobenius.

Suppose G is Frobenius. By Lemmas 5 and 6, we know that either G is solvable or a Sylow 2-subgroup of G is generalized quaternion. We arrive at $t(G) \leq 2$ by Lemma 7. This contradicts our assumption.

The case when G is 2-Frobenius is similar.

Case 2. G is simple.

The assertion follows with Theorem A.

Case 3. G is an extension of a nontrivial π_1-group by a simple group.

In this case, there exists a normal π_1-subgroup N of G such that G/N is simple. Since $t(G) \geq 3$, N admits a fixed-point-free automorphism of prime order. By Lemma 5, N is nilpotent. Note that $|\pi(G) - \pi(G/N)|$ is the number of vertices that lie in $\pi_1(G)$ but not in $\pi_1(G/N)$. Since $2 \notin \pi(G) - \pi(G/N)$, by Lemma 3 we have that $|\pi(G) - \pi(G/N)|$ is at most the number of edges that are in the component $\pi_1(G)$ but not in $\pi_1(G/N)$. Evidently the latter is at most the number $\psi(G) - \psi(G/N)$. Hence we have an inequality

$$|\pi(G) - \pi(G/N)| \leq \psi(G) - \psi(G/N). \tag{1}$$

By Theorem A we have another inequality

$$|\pi(G/N)| \leq \psi(G/N) + 3. \tag{2}$$

So

$$\begin{aligned}|\pi(G)| &= |\pi(G) - \pi(G/N)| + |\pi(G/N)| \\ &\leq (\psi(G) - \psi(G/N)) + (\psi(G/N) + 3) = \psi(G) + 3.\end{aligned}$$

It is clear that the equality $|\pi(G)| = \psi(G) + 3$ holds if and only if both equalities in (1) and (2) hold.

If $\pi(N) \subseteq \pi(G/N)$, then $\pi(G) = \pi(G/N)$. Hence $\psi(G) = \psi(G/N)$, and further $\pi_e(G) = \pi_e(G/N)$. That the inequality in (2) holds implies that G/N is one of the simple groups listed in Theorem A. From [2, 13–15], we have that G is isomorphic to G/N, i.e., $N = 1$, a contradiction as $N \neq 1$ by assumption.

If $\pi(N) \nsubseteq \pi(G/N)$, we will get a contradiction too.

(1) If $r \in \pi(G) - \pi(G/N)$ then $2r \in \pi_e(G)$. Otherwise a Sylow 2-subgroup of G is cyclic or a generalized quaternion group. By Lemma 7 we now get $t(G) \leq 2$, a contradiction.

(2) $\pi(G) - \pi(G/N) = \{r\}$, $r \neq 2$. Let $r \in \pi(G) - \pi(G/N)$. Suppose $|\pi(G) - \pi(G/N)| \geq 2$. Put $r \neq s \in \pi(G) - \pi(G/N)$. Consider G/S, where S is a Sylow s-subgroup of N (also G). On the one hand, $|\pi(G)| = |\pi(G/S)| + 1$. By statement 1, $2s \in \pi_e(G)$. Since N is nilpotent, $rs \in \pi_e(G)$. Furthermore, we have $\psi(G) \geq \psi(G/S) + 2$. On the other hand, $|\pi(G/S)| \leq \psi(G/S) + 3$ holds by induction on G/S. Hence

$$|\pi(G)| = |\pi(G/S)| + 1 \leq \psi(G/S) + 4 \leq \psi(G) + 2,$$

which contradicts $|\psi(G)| = \psi(G) + 3$.

(3) $\pi_e(G) - \pi_e(G/N) = \{r, 2r\}$. From statement 2, we have $\psi(G) - \psi(G/N) = 1$. By statement 1, $2r \in \pi_e(G)$. From statement 2 we have the conclusion statement 3.

(4) $C_G(R) \subseteq R$, where R is a Sylow r-subgroup of N. Clearly R is also a Sylow r-subgroup of G. Considering G/R, from statements 2 and 3 we get that $|\pi(G/R)| = \psi(G/R) + 3$. By induction on G/R, we have that G/R is simple. Since G/N is simple, we know that $N = R$. So we have $C_G(R) \subseteq R$.

(5) We finally get a contradiction. Assume there is some elementary abelian 2-subgroup H in G/R on which some element x of prime order acts irreducibly. Then by statement 3, x acts fixed-point-freely on R. Hence it acts fixed-point-freely on the preimage of H, which is nilpotent by Lemma 5. However, this contradicts $C_G(R) \subseteq R$. The groups $L_2(2^n)$ and $\mathrm{Sz}(2^n)$ contain groups of order $2^n(2^n - 1)$ by [10, Chap. 11]. The group J_1 contains a group of order $8 \cdot 7$ by [4] and $L_3(4)$ and $L_2(q)$ contain A_4, so we are done.

Case 4. G is an extension of a simple group by a nontrivial π_1-group.

In this case, there exists a simple normal subgroup N of G such that G/N is a π_1-group. Since $t(G) \geq 3$, we have $t(N) \geq 2$. Hence $C_G(N) = 1$.

Therefore, $N \leq G \leq \mathrm{Aut}(N)$. By induction on N, we have an inequality

$$|\pi(N)| \leq \psi(N) + 3 \tag{3}$$

and the equality holds if and only if N is one of the simple groups listed.

According to a reason similar to the first lines of the proof in Case 3, we have an inequality

$$|\pi(G) - \pi(N)| \leq \psi(G) - \psi(N) \tag{4}$$

by Lemma 3. So

$$|\pi(G)| = |\pi(G) - \pi(N)| + |\pi(N)| \leq \psi(G) + 3,$$

and $|\pi(G)| = \psi(G) + 3$ holds if and only if the equalities in (3) and (4) hold.

First, assume that $\pi(G) = \pi(N)$. We have then that $|\pi(G)| = |\pi(N)| \leq \psi(N) + 3 \leq \psi(G) + 3$. If $|\pi(G)| = \psi(G) + 3$ holds, then $\psi(N) = \psi(G)$. Hence $\pi_e(N) = \pi_e(G)$. By [2, 13–15], we have that G is isomorphic to N, a contradiction.

Second, assume that $\pi(G) \neq \pi(N)$. Note that the simple groups mentioned below are from Theorem A.

(1) N is isomorphic to either J_1 or $L_3(4)$. From [4], $\mathrm{Out}(J_1) = 1$, we have a contradiction. If N is isomorphic to $L_3(4)$, then $\mathrm{Out}(L_3(4)) = \mathbb{Z}_2 \times S_3$ by [4]. Clearly $\pi(G) = \pi(N)$ (see [4, p. 23]), a contradiction as $\pi(G) \neq \pi(N)$.

(2) N is isomorphic to $L_2(q)$, $q = p^n$. It is well known that $\mathrm{Aut}(L_2(p^n)) = PGL_2(p^n) : \mathbb{Z}_n$. First, assume $p > 2$. When $n = 1$, $\mathrm{Aut}(N) = PGL_2(q)$. So $\pi(G) = \pi(N)$. This contradicts $\pi(G) \neq \pi(N)$. When $n \geq 2$, $p = 3$ or 5 by Theorem A. By [7, Theorem 4.23, p. 304], the group of diagonal automorphisms of order 2 is normal in $\mathrm{Out}(N)$. Hence, the diagonal automorphism commutes with the field automorphism. Since n is odd, $\mathrm{Out}(N) = \mathbb{Z}_2 \times \mathbb{Z}_n$. As $\pi(G) \neq \pi(N)$ there is some field automorphism of prime order r in G. However, this automorphism centralizes some element of order p in G. So r is connected to p in the prime graph, i.e., $p \in \pi_1(G)$. As $p \notin \pi_1(N)$ this now implies $t(G) \leq 2$, a contradiction. Second, assume $p = 2$. We have $\mathrm{Aut}(N) = L_2(2^n) : \mathbb{Z}_n$. Let $g = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in L_2(2^n)$. Clearly the order of g is 3. On the one hand, as $\pi(G) \neq \pi(N)$ there is some field automorphism of prime order r in G. On the other hand, his automorphism centralizes the element g. Hence $3r \in \pi_e(G)$. We have $t(G) \leq 2$ as above, a contradiction.

(3) N is isomorphic to $Sz(q)$, $q = 2^{2n+1}$. It is well known that $\mathrm{Aut}(Sz(q)) = Sz(q):\mathbb{Z}_{2n+1}$. Without loss of generaity, we may assume $G = Sz(q):\mathbb{Z}_{2n+1}$. Take

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

From [6], $x \in Sz(q)$. Clearly $|x| = 4$. Let τ: $\alpha \to \alpha^2$ be a field automorphism of $GF(q)$. Since $x^\tau = x$ and the order of τ is odd, G has an element of order $4(2n+1)$. G also has an element of order $2(2n+1)$. So $\psi'(G) \geq 2$. By Lemma 1, $|\pi(G)| < \psi(G) + 3$, a contradiction.

Case 5. G is an extension of a nontrivial π_1-group by a simple group by a nontrivial π_1-group.

In this case, there exists normal subgroups N and G_1 of G such that $1 < N < G_1 < G$, N is a π_1-group, G_1/N is simple, and G/G_1 is a π_1-group. By the inductive hypothesis, $|\pi(G_1)| \leq \psi(G_1) + 3$, and further as G_1 is not simple we have $|\pi(G_1)| < \psi(G_1) + 3$. If $\pi(G) = \pi(G_1)$, then $|\pi(G)| < \psi(G_1) + 3 \leq \psi(G) + 3$ holds. If $\pi(G) \neq \pi(G_1)$, then $|\pi(G) - \pi(G_1)| \leq \psi(G) - \psi(G_1)$ by Lemma 3. So

$$\begin{aligned} |\pi(G)| &= |\pi(G) - \pi(G_1)| + |\pi(G_1)| \\ &< \big(\psi(G) - \psi(G_1)\big) + \big(\psi(G_1) + 3\big) \\ &= \psi(G) + 3, \end{aligned}$$

i.e., in Case 5 we always have inequality $|\pi(G)| < \psi(G) + 3$.

This completes the proof of Theorem B.

ACKNOWLEDGMENT

Both authors are grateful to the referee for kind help in modifying the original version of the paper.

REFERENCES

1. N. Bourbaki, "Groupes et Algebres de Lie," Chaps. 4–6, Hermann, Paris, 1968.
2. R. Brandl and Shi Wujie, The characterization of PSL$(2, q)$ by its element orders, *J. Algebra* **163** (1994), 109–114.
3. R. Brauer and M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group, *Proc. Nat. Acad. Sci. USA* **45** (1959), 1757–1759.
4. J. H. Conway et al., "ATLAS of Finite Groups," Clarendon Press, Oxford, 1985.

5. M. Deaconescu, Classification of finite groups with all elements of prime order, *Proc. Amer. Math. Soc.* **106**, (1989), 625–629; K. N. Cheng, M. Deaconescu, M. L. Lang, and W. J. Shi, Corrigendum and addendum to Classification of finite groups with all elements of prime order, *Proc. Amer. Math. Soc.* **117** (1993), 1205–1207.
6. D. Gorenstein, "Finite Groups," Harper and Row, New York, 1982.
7. D. Gorenstein, "Finite Simple Groups, An Introduction to their Classification," Plenum Press, New York, 1982.
8. K. W. Gruenberg and O. H. Kegel, unpublished manuscript, 1975.
9. G. Higman, Finite groups in which every element has prime order, *J. London Math. Soc.* **127** (1957), 335–342.
10. B. Huppert and N. Blackburn, "Finite Groups III," Springer-Verlag, Berlin, 1982.
11. N. Iiyori and B. Yamaki, Prime graph components of the simple groups of Lie type over the field of even characteristic, *J. Algebra* **155** (1993), 335–342.
12. H. Kurzweil, "Endliche Gruppen," Springer-Verlag, Berlin, 1977.
13. W. J. Shi, A characterization of some projective special linear groups, *J. Math. (PRC)* **5** (1985), 191–200.
14. W. J. Shi, A characteristic property of J_1 and $PSL_2(2^n)$, *Adv. in Math.* **16** (1987), 397–401 (in Chinese).
15. W. J. Shi, A characterization of Suzuki's simple groups, *Proc. Amer. Math. Soc.* **114** (1992), 589–591.
16. W. J. Shi, A class of special finite groups, *Northeast Math. J. (China)* (1993), 1–4.
17. W. J. Shi and Y. Wenze, A new characterization of A_5 and the finite groups in which every non-identity element has prime order, *J. Southwest China Teachers College* **1** (1984), 36–40 (in Chinese).
18. W. J. Shi and C. Yang, A class of special finite groups, *Chinese Sci. Bull.* **36** (1991), 1275.
19. M. Suzuki, "Group Theory I," Springer-Verlag, Berlin, 1982.
20. H. N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62–89.
21. J. S. Williams, Prime graph components of finite groups, *J. Algebra* **69** (1981), 487–513.